

INTRODUCTION

By way of their instant Motion to Dismiss, Defendants seem to believe that they assemble their Smart TVs with some sort of magic – “legal proof” – glass and components, and that Defendants are simply not subject to federal or state law. The law, these foreign-based entities insist¹, allows this Court to do nothing to stop the sophisticated snare Defendants have laid down for unsuspecting consumers. Rather, Defendants contend they can lure consumers with features such as video libraries on-demand, Netflix, Amazon, Hulu, and Pandora, and other enticing applications and, once consumers take the bait, Defendants are then able follow these unsuspecting consumers deep into the private, confidential areas of their lives.

As alleged thoroughly in Plaintiffs’ Amended Class Action Complaint (the “Complaint” or “Compl.”), using state-of-the-art technology, encryption techniques and data aggregation experts, Defendants secretly track and store everything consumers watch, everything consumers say, as well as the specific identifiers (and thus the real world location) of other electronic devices that consumers connect to their Smart TVs and/or Wifi. Compl. ¶¶ 41-69. Defendants are then able to sell this confidential, personally-identifying information and the private viewing habits of consumers to data brokers and advertisers. Compl. ¶¶ 4, 20-21, 120. Defendants do this without obtaining consumers informed consent, and they are able to track and record consumers indefinitely. Compl. ¶¶ 9-10, 45, 60-61, 67, 92, 101, 105. Defendants do not even attempt to deny that they engage in the brokering of consumers’ confidential and personal information.

¹ The “parent” company of each Defendant is located outside the United States. In the modern world of electronic storage, logic dictates that the confidential, private information that Defendants unlawfully siphon from Smart TV users is also stored and transferred by Defendants to foreign servers located outside of the United States.

But the law is not so submissive. State legislatures and the United States Congress have enacted privacy statutes that apply directly. While many of these laws were passed before the modern era of “big data” analytics, video streaming, and data-voice recognition, that has no concern here, as “[d]rafters of every era know that technology advances will proceed apace and that the rules they create will one day apply to all sorts of circumstances they could not possibly envision.” Scalia and Garner, *Reading Law: The Interpretation of Legal Texts* 85-86 (2012). These privacy and other statutes limit Defendants’ legal right to collect or disclose consumers’ personal and/or identifying information without informed consent, and Defendants’ failure to secure that informed consent renders them liable for damages. See, e.g., Nickelodeon Cons. Priv. Litig., 827 F.3d at 290 (3d Cir. 2015). See also United States v. Shultz, 2018 U.S. Dist. LEXIS 11295 (10th Cir. 2017); In re Defendants, Inc. Consumer Privacy Litig., 238 F. Supp. 3d 1204 (C.D. Cal. 2017). Accord In re Horizon Healthcare Servs., Inc. Data Breach Litig., 846 F.3d 625, 638-641 (3d Cir. 2017) (citing Spokeo, Inc. v. Robins, 136 S.Ct. 1540 (2016)) (holding alleged violation of federal privacy statute resulting in disclosure of personal information to third party was sufficient for standing in data breach case and holding “improper dissemination of information can itself constitute a cognizable injury”).

In addition to Defendants’ violation of a litany of privacy laws, consumer protection, tort,² and contract law also broadly prohibit the unfair and illegal business practices used by Defendants here. Again, Defendants do not deny their actions with regard to tracking, recording, and storing consumers’ private, confidential information and watching habits; rather, Defendants’ challenges to those laws are largely limited to an incorrect attempt at pleading technicalities. But, like it or not,

² As articulated by the American Law Institute in its First Restatement of Torts, an invasion of privacy constitutes an “unreasonabl[e] and serious[] interfere[nce] with another’s interest in not having his affairs known to others or his likeness exhibited to the public . . .” . See Restatement (First) of Torts § 867 (1939).

United States law holds each individual and entity accountable for their misconduct and – wish as they may – Defendants cannot simply foreclose this Court’s consideration of the merits of Plaintiffs’ claims. The motion to dismiss should be denied in its entirety.

FACTS

Defendants are amongst the largest manufacturers in the world of "Smart TVs," cutting-edge televisions equipped with integrated software that enables consumers to access, amongst other things, the internet and instant, on-demand video services. Compl. ¶¶ 35-36. Defendants’ Smart TVs stream video and other content to consumers, and allow consumers to access WiFi networks to gain access and watch various forms of audio and visual entertainment online, as well as to find access to online news, weather, and entertainment sources. Compl. ¶¶ 36-37. To accomplish this, Defendants’ Smart TVs are delivered to consumers with many pre-installed applications, and other applications are uploaded by Defendants to their Smart TVs. These include such popular internet applications as Netflix, YouTube, Amazon, Pandora, Hulu, Twitter, and more. The list is ever-growing. Compl. ¶ 38.

Defendants’ business model, however, is much more than selling TVs. In reality, due to fierce market competition, Defendants reap extremely slim profit margins on TV sales. To offset this, Defendants use Automatic Content Software (“ACS”) to capture, in real time, viewing data, watching habits, other personally-identifiable information, and the voices from the users of their Smart TVs. Compl. ¶¶ 41-69. Defendants collect, aggregate, and store data for most of the content viewed on their Smart TVs – and also the other devices connected to the consumers’ Wifi (such as cable and satellite providers, gaming consoles, DVD players, and other sources). Compl. ¶¶ 38, 49, 57, 154. Defendants then sell this data to third-party advertisers and media content providers, who also use (and store) this private

information to target consumers. See, e.g., Compl. ¶¶ 4-5, 44, 43, note 16, note 38. Throughout the process, Defendants also collect a wide array of additional information about consumers' watching habits and views, including their IP addresses, zip codes, online services used, MAC addresses, and much more identifying information. Compl. ¶¶ 49, 52, 56. The date and time of users viewing and search history is also collected, see, e.g., Exhibit 1 attached to the Amended Complaint -- and a data "fingerprint" is created by Defendants for each individual Smart TV user in the home. Compl. ¶¶ 44, 49, 52, 56, note 19.

Defendants accomplish their pirating of consumers' confidential information and voice recordings by employing the services of sophisticated data processors and information-recognition companies, such as Cognitive Networks, whose only business purpose is to accomplish exactly what Plaintiffs have alleged. See, e.g., Compl. ¶¶ 4-5, 44, 43, note 16, note 38. See also Exhibit 1 to the Complaint (*Automatic Content Software materials*). As Zeev Neumeier, Cognitive Network's Founder and President, explained, third-party data-recognition companies that Defendants employ to collect private confidential information and watching habits about consumers utilize ACS technology that "[L]ooks at the picture on your TV and uses that data to identify exactly what you're watching." Compl. ¶5³

Defendants' data and voice-recording collection and transmission is, by intention, unbeknownst to consumers. See, e.g., Compl. ¶¶ 1-4, 6, 9, 11, 41, 42-47, 64-68. And because of that fact, there could be no informed consent in this case.⁴

³ See also Exhibit 1 attached to the Amended Complaint (Automatic Content Software Platform Diagram).

⁴ "In reality, Defendants conceal their A[utomatic] C[ontent] S[oftware 'ACS'] and the method for disabling it. In order not to be subjected to Defendants ACS and monitoring programs forever, the consumer must somehow – while taking the unit out of a cardboard box and attempting to physically install it (or, as is often is the case, having someone else set it up for the consumer):

- a. find the privacy policy, read and comprehend the complex legal text;
- b. understand how, why, when, and if Defendants are collecting confidential information about them;
- c. determine whether or not Defendants' data collection is for Defendants' profit;
- d. figure out if Defendants are monitoring and collecting their personal information in real time;
- e. try to compute how much information Defendants are collecting and from which devices; and

Nowhere in the packaging or marketing of Defendants' Smart TVs do Defendants disclose its data and voice collection practices (and that Defendants sell that information to third parties, who also store that sensitive information). Compl. ¶¶ 61-62. Even though it would be simple and no-cost for Defendants to alert consumers on the television box itself (*ie*; prior to the purchase of the TV by the consumer) that Defendants collect and store indefinitely consumers' highly-sensitive, personal and confidential information and voices (and that Defendants then sell this confidential information to third parties), *Defendants do not print this material information on the television box*. Even though it would be simple and no-cost for Defendants to put in bold print (or any print) in the instruction manual in the box that Defendants collect and store indefinitely consumers' highly-sensitive, personal and confidential information and voices (and that Defendants then sell this confidential information to third parties), *Defendants do not print this material information on in the instruction manual in the box*. Even though it would be simple

f. determine if Defendants are storing consumers' private information on their servers, and for how long. . . .

Then, consumers must figure out:

- i. when and if Defendants are transmitting their information to outside third parties,
- ii. how much information they are transmitting to third parties and for what purposes,
- iii. to what third parties they are transmitting consumer information to, and what the privacy policies of the outside third parties are; and

iv. whether the third parties are storing consumers' private information on their servers, and for how long. . . .

Consumers must further figure out:

- a. if those outside third parties are transmitting their personal information to other outside "second level" third parties, and

b. to what 'second level' third parties Defendants are transmitting consumer information to;

c. how much information they are transmitting to 'second level' third parties and for what purposes;

d. what the privacy policies of the outside 'second level' third parties are; and

e. whether the 'second level' third parties are storing consumers' private information on their servers, and for how long. . . .

Furthermore, Defendants' customers do not have access to the names of the outside third parties (or outside 'second level' third parties) or access to the separate privacy policies of these outside parties (or outside 'second level' third parties) or access to the licensing agreements between Defendants and these third parties.

Compl. ¶¶ 63-65, 67. Thus, there can be no informed consent by consumers here because they are not reasonably provided with all the facts to make an informed decision. Id.

and no-cost for Defendants to put a conspicuous, separate and bold **“Privacy Information Sheet”** in the box that explains how and why Defendants collect (and store indefinitely) consumers’ highly-sensitive, personal and confidential information and voices (and that Defendants then sell this confidential information to third parties), *Defendants do not include any conspicuous “Privacy Information Sheet” inside the box.* See Compl. ¶ 11 (“Plaintiffs and the proposed Class Members did not know about and did not consent to Defendants’ placement and/or use of Automatic Content Software inside the Smart TVs they purchased, and/or Defendants’ tracking and/or recording of Plaintiffs and the Class via Defendants’ Smart TVs, and/or Defendants transmission of private consumer information and voices to third parties, and/or Defendants transmission of private consumer information and voices to third parties for profit.”); ¶¶21-22.

The data and voice collection by Defendants also allows that information to be used in order to identify specific people in the home (including children), compl. ¶¶ 87-89, and connect them with what they have been watching and where they live. For example, Plaintiffs allege that Defendants scan consumers’ Wifi system. Compl. ¶¶ 38, 49, 57, 154. Plaintiffs also allege that Defendants video-streaming platforms disclose substantial, extensive information about Plaintiffs’ and consumers’ “digital identities”; namely, consumers’ video-viewing history, consumers’ computer addresses, and other information about other devices connected to the same Wifi network. See Id. See also Compl. ¶¶ 49, 52, 56.⁵ That alone satisfies the VPPA pleading standard laid down by the Third Circuit in In re Nickelodeon Cons. Priv. Litig., 827 F.3d at 290 (3d Cir. 2015). See infra.

⁵ Further, users can be asked by certain applications on Smart TVs to sign up for services requiring their name and email address, which makes it especially easy for third parties to identify consumers’ viewing habits.

The named Plaintiffs in this case bought Defendants’ Smart TVs with no inkling of the fact that Defendants would be monitoring and disclosing everything they watch and say – let alone that Defendants would be selling and transmitting their private, confidential, identifying information to third parties, for profit. Compl. ¶¶ 11, 21-22. Although, like every purchaser of a Smart TV in a retail store, Plaintiffs examined Defendants’ packaging when they were shopping for their Smart TVs and noted features such as the TVs’ ability to connect to the internet and stream content from many sources, Plaintiffs did not see – because Defendants failed to properly disclose – any indication that their viewing data, personally-identifiable information, and voice content would be collected, stored by Defendants, and sold to third parties. *Id.* With Plaintiffs having no idea of the scheme Defendants had cooked-up to invade, store, and sell their private and identifying information (and for other reasons), Plaintiffs did not – and could not – give informed consent to the unlawful collection by Defendants of their private information and/or Defendants’ disclosure of this information to third parties for profit. *See also, supra*, note 4. Had Plaintiffs and the Class members known the truth, they would have not purchased Defendants’ Smart TVs, or would have paid substantially less. Compl. ¶ 11.

ARGUMENT

I. Plaintiffs’ Statutory Privacy Claims Are Well-Pled

Plaintiffs have adequately pled their statutory privacy claims.

A. Plaintiffs’ VPPA Claims Are Well Pled

Enacted in 1988, the Video Privacy Protection Act (“VPPA”) provides that “[a] *video tape service provider* who knowingly discloses, to any person, *personally identifiable information* concerning any *consumer* of such provider shall be liable to the aggrieved person” 18 U.S.C. § 2710(b)(1); Video Privacy Protection Act of 1988, S. 2361, 100th Cong., 102 Stat. 3195 (1988) (emphasis added). The Act allows

consumers “to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers.” S. Rep. No. 100-599 at 8 (1988). The VPPA also protects consumers by requiring that their consent be obtained before their personal video-viewing histories can be divulged.

Defendants seek to dismiss Plaintiffs’ VPPA claims, arguing that they are not “video tape service provider[s],” that Plaintiffs are not “consumer[s]” as defined by the statute, and that Defendants do not disclose “personally identifiable information.” Each argument misreads the VPPA; the instant Complaint; and the Third Circuit’s (and other courts’) interpretation of the statute.⁶

1. Defendants Are “Video Tape Service Providers”

Defendants deliver through Smart TV software streaming video directly to consumers homes through the software that Defendants developed for its Smart TVs. Compl. ¶¶ 39, 54. Using Defendants’ platforms, the user can select videos from various video libraries, including Hulu’s, Amazon’s and Netflix’s, for instant delivery. *Id.*⁷ By using Defendants’ video-delivery software service, Defendants collect certain private information about the user. Compl. ¶¶ 41-69.

Against this backdrop, Plaintiffs have properly alleged that each Defendant qualifies as a “video tape service provider” because it is a “person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or *similar audio visual materials*[.]” 18 U.S.C. § 2710 (emphasis added). That is, the Complaint precisely alleges that each Defendant

⁶ “[W]hen [a] statute’s language is plain, the sole function of the courts – at least where the disposition required by the text is not absurd – is to enforce it according to its terms.” *Lamie v. U.S. Tr.*, 540 U.S. 526, 534 (2004) (quoting *Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A.*, 530 U.S. 1, 6 (2000)). “The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which the language is used, and the broader context of the statute as a whole.” *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997).

⁷ In this regard, Defendants compete directly with other video delivery services, such as Roku. *See* https://article.wn.com/view/2018/01/17/Roku_Introduces_New_Metrics_for_OTT_Advertising_Campaigns/

is not merely a television manufacturer; they also clearly provide consumers with a service: *the delivery of streaming video* (*i.e.*, “*similar audio visual materials*”) through their Smart TV platforms. Indeed, Plaintiffs (like virtually every purchaser of a Smart TV) purchased their Smart TVs in part because Defendants’ technology brings the video rental store into the home, allowing Plaintiffs to access video on demand through Defendants’ Smart TV interface.⁸

Defendants contend they are not video tape service providers under the VPPA. However:

The plain text of the statute provides otherwise. As an initial matter, Congress’s use of a disjunctive list (*i.e.*, ‘engaged in the business . . . of . . . rental, sale, or delivery’) unmistakably indicates that Congress intended to cover more than just the local video rental store. Indeed, lest the word ‘delivery’ be superfluous, a person need not be in the business of either renting or selling video content for the statute to apply. Further, Congress’s use of the phrase ‘similar audiovisual materials’ indicates that the definition is medium-neutral; the defendant must be in the business of delivering video content, but that content need not be in a particular format.

In re Vizio, Inc., 238 F. Supp. 3d 1204, 1221. See also In re Hulu Privacy Litig., No. C 1103764 LB, 2012 WL 3282960, at *5 (N.D. Cal. Aug. 10, 2012). Accord In re Nickelodeon Cons. Priv. Litig., 827 F.3d at 290 (3d Cir. 2015).

As the statutory text supports Plaintiffs’ position -- not Defendants’ -- so does the legislative history. The VPPA was of course enacted before this type of

⁸ Companies like Hulu, which are accessible through Defendants’ video-delivery software, are not the only “video tape service providers” within the arrangement. The VPPA simply asks whether an interstate business is engaged in the delivery of “similar audio visual materials,” which includes streaming video. See In re Hulu Privacy Litig., 2012 WL 3282960, at *5-*6 (N.D. Cal. Aug. 10, 2012) (holding Hulu qualified as a “video tape service provider” because it helped deliver television and movies through the Internet for free). Instead, under a plain reading of the statute, any company that provides this service must obtain informed consent before disclosing individuals’ personal viewing-histories and confidential, identifying information.

technology existed, but “Congress was concerned with protecting the confidentiality of private information about viewing preferences *regardless* of the business model or media format involved.” Hulu, 2012 WL 3282960, at *6 (emphasis added). Congress may not have imagined the technology Defendants have developed to deliver streaming video through licensing agreements with content providers like Hulu, but it “cast such a broadly inclusive net in the brick-and-mortar world, [that there is] no reason to construe its words as casting a less inclusive net in the electronic world when the language does not compel that we do so.” See Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 488 (discussing “subscriber”).

Thus, in addition to the fact that, on its face, each Defendants clearly provide an in-home video delivery service to consumers, Congress’s choice of language in defining *video tape service provider* also fairly brings Defendants’ video-delivery service within the VPPA, and therefore “it is unimportant that the particular application may not have been contemplated by the legislators.” Barr v. United States, 324 U.S. 83, 90 (1945).

Accordingly, the VPPA’s protections plainly *do* apply to a business that runs a video-delivery service through software designed to bring the video-rental store into the home—which is precisely why each Defendants *is* a qualifying “video tape service provider.”

2. Plaintiffs are subscribers and hence consumers.

Next, Defendants argues that Plaintiffs are not “consumers” under the VPPA. The statute defines “consumer” to include a “subscriber” of goods or services from a video tape service provider. 18 U.S.C. § 2710(a)(1). Though the word subscriber is not defined therein, its ordinary meaning includes one who receives electronic texts or services by subscription. Yershov, 820 F.3d at 487.

In Yershov, the First Circuit held that an individual who accesses news and entertainment media content, including videos, through a proprietary mobile software application on his mobile phone qualifies as a “subscriber” within the meaning of the VPPA. The app was free, but the court rejected the argument that monetary payment is necessary to qualify as a subscriber. 820 F.3d at 487. Instead, it found that the use of the mobile app generated information about that user that the defendant collected, and this was sufficient to establish a subscriber relationship. Id.; see also Hulu, 2012 WL 3282960, at *8 (concluding plaintiffs were subscribers of Hulu, notwithstanding that they watched videos on Hulu for free, in part because Hulu collected their data in exchange for viewing).⁹

Simply put, Plaintiffs here used Defendants’ proprietary Smart TV platform to watch video, and Defendants collected and sold (and continue to collect and sell) Plaintiffs’ and consumers’ personal data when they do, such as computer addresses and the addresses of other electronic items connected to Wifi, and what, where and when consumers watch -- which can be then be used (and are used) by Defendants, with the help of data aggregators, to reveals the *electronic location* of Defendants’ and other devices connected to Plaintiffs’ Wifi (i.e., geolocation data). Compl. ¶¶ 38, 49, 57, 154. Defendants also collect this data so that they can push personalized ads to their devices as well as consumers’ *other* devices. Compl. ¶¶ 45-47. “[A]ccess was not free of a commitment to provide consideration in the form of that information, which was of value to” Defendants. See Yershov, 820 F.3d at 489. And it was not free in a different sense: Defendants sell Smart TVs with this “streaming video” technology (at a premium) in order to allow consumers to have regular, and

⁹ In Yershov, the First Circuit concluded that a consumer need not make a monetary payment in return for a mobile application to be considered a “subscriber.” 820 F.3d 482, 488-89 (1st Cir. 2016). Instead, the plaintiff’s provision of personal information in return for the defendant’s video content was sufficient consideration for the plaintiff to be a “subscriber.” Id. at 489. See also In re Vizio, Inc., 238 F. Supp. 3d 1204.

easy, access to video delivery services in their homes. Ironically and absurdly, all along Defendants were and are secretly using those same delivery services to reap millions of dollars off the personal, private information from unsuspecting consumers.

In these ways, Plaintiffs have alleged a sufficient relationship with Defendants' video delivery services, such that Plaintiffs are clearly "subscribers" under the VPPA.

3. Defendants Disclosed Plaintiffs' and Class Members' "Digital Identities" Constituting Personally Identifiable Information.

The VPPA provides that "the term 'personally identifiable information' includes information which identifies a person . . ." § 2710(a)(3) (emphasis added). Unlike other definitions of "personally identifiable information" which list specific types of data as qualifying, this is an example of a "standard" which is "open rather than closed in nature" and "can evolve and remain flexible in response to new developments." Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814 (2011). That Congress chose to define "personally identifiable information" in terms of a standard is evident from its use of the word "includes." This word "normally implies that the proffered definition falls short of capturing the whole meaning." Yershov, 820 F.3d at 486; see also United States v. Gertz, 249 F.2d 662, 666 (9th Cir. 1957) ("The word 'includes' is usually a term of enlargement, and not of limitation."). The legislative history confirms this reading. Id. (noting "official Senate Report expressly stating that the drafters' aim was 'to establish a minimum, but not exclusive, definition of personally identifiable information.'" (quoting S. Rep. No. 100-599, at 12))).

Congress’s approach makes great sense for two reasons. For one, “many types of information other than a name can easily identify a person.” 820 F.3d at 489.¹⁰ It can depend on the context. “[W]hen a football referee announces a violation by ‘No. 12 on the offense,’ everyone with a game program knows the name of the player who was flagged.” *Id.* For another, the ability of any given information to identify individuals may change over time. 86 N.Y.U. L. Rev. at 1836.

Here, Plaintiffs allege that Defendants video-streaming platforms disclose substantial, extensive information about Plaintiffs’ and consumers’ digital identities; namely, consumers’ video-viewing history, consumers’ computer addresses, and information about other devices connected to the same Wifi network. Compl. ¶¶ 45-47. That alone satisfies the VPPA pleading standard laid down by the Third Circuit in *In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d at 290 (3d Cir. 2015).

Moreover, the court in *Vizio* – a similar case as to this one – explained why VPPA claims there were be upheld under the standard laid down by the Third Circuit in *Nickelodeon*:

The Court need not disagree with *In re Nickelodeon* because Plaintiffs allege that Vizio’s Inscape platform discloses even more about their digital identities—in particular, consumers’ MAC addresses and information about other devices connected to the same network. Plaintiffs allege that MAC addresses are frequently linked to an individual’s name and can be used to acquire highly specific geolocation data. (Compl. ¶¶ 69-71.) MAC addresses allegedly can also identify a person when combined with Vizio’s disclosure of consumers’ IP addresses, zip codes, product model numbers, hardware and software versions, chipset IDs, and region and language settings. (*Id.* ¶¶ 72-79.) Besides collecting and

¹⁰ “Congress contemplated that the Act would protect more than just a person’s name or physical address.” *See also In re Vizio, Inc.*, 238 F. Supp. 3d 1204, 1224. Besides collecting and disclosing extensive information regarding consumers’ Smart TVs, Plaintiffs allege that Defendants collect and disclose information about all other devices connected to the same network. *See, e.g.*, Compl. ¶¶ 45-47.

disclosing extensive information regarding consumers' Smart TVs, Vizio supposedly collects and discloses information about all other devices connected to the same network. (Id. ¶¶ 63, 72.)

In re Vizio, Inc., 238 F. Supp. 3d 1204, 1224. See also Yershov, 820 F.3d at 489.

Here, Plaintiffs have made similar allegations, and the same reasoning applies.¹¹

Plaintiffs' allegations also detail how this information links viewing data to specific individuals, including the creating by Defendants of a digital "fingerprint" of every user in a home and Defendants' ability to scan a users' Wifi network. Compl. ¶¶ 44, 49, 52, 56, note 19. Plaintiffs describe how addresses are unique to Plaintiffs' Smart TVs and consumers' other electronic devices. Id. Plaintiffs allege Defendants disclose this data for not only the Smart TVs themselves, but all media sources connected to consumers' Wifi. Compl. ¶¶ 38, 49, 57, 154. These allegations also plausibly state a claim under the VPPA. Nickelodeon, 827 F.3d at 290. See also Yershov, F. Supp. 3d at 135; In re Vizio, Inc., 238 F. Supp. 3d 1204, 1225.¹²

Further, the Complaint alleges Defendants disclose other personally identifiable information that is "reasonably and foreseeably likely to reveal which" videos Plaintiffs obtained. Compl. §§ 46-48. See also Yershov, 820 F.3d at 486; In re Vizio, Inc., 238 F. Supp. 3d at 1224 ("The First Circuit in Yershov concluded that *personally identifiable information* . . . embrace[s] "information reasonably and foreseeably likely to reveal which . . . videos [the plaintiff] has obtained.")). 820 F.3d at 486.

¹¹ Of course, discovery will hopefully allow for details concerning how extensive Defendants' were collecting and disclosing (and are currently collecting and disclosing) private consumer information and information about all other devices connected to consumers' Wifi networks.

¹² In addition, the Complaint alleges Defendants disclose other personally identifiable information that is "reasonably and foreseeably likely to reveal which" videos Plaintiffs obtained. See Yershov, 820 F.3d at 486. See also In re Vizio, Inc., 238 F. Supp. 3d 1204, 1224 ("The First Circuit in Yershov concluded that "personally identifiable information" extends beyond a person's name to embrace "information reasonably and foreseeably likely to reveal which . . . videos [the plaintiff] has obtained.")).

Defendants argue that this is not what they are doing and ask the Court to hold that the confidential and identifying personal information about consumers that Defendants steal, store, and sell to third parties (*i.e.*, specific information that identifies what a user watches; how long a user watches; and where they watch videos, as Plaintiffs allege) (*see, e.g.* Exhibit 1 attached to the Complaint) does not violate the VPPA *as a matter of law*. As Defendants know and explained in detail above, this factual argument and inquiry – a dispute of scientific fact – and is entirely improper in a technology case at the pleadings stage. *See E.digital Corp. v. Toshiba Am. Info. Sys., Inc.*, 2014 WL 12516081, at *3 (S.D. Cal. July 10, 2014). “[S]uch arguments are better suited for a motion for summary judgment on a more developed record.” *E.digital Corp.*, 2014 WL 12516081, at *3. *See also In re Vizio, Inc.*, 238 F. Supp. 3d 1204, 1225.¹³

The Court should also not accept Defendants’ offer to engage in judicial fact-finding or make sweeping determinations as a matter of law on this Motion to Dismiss. *Yershov*, 104 F. Supp. 3d at 145 (“the factual record would need to be developed before concluding that an Android ID is not PII”); *In re Hulu Privacy Litig.*, 2012 WL 3282960, at *7 (N.D. Cal. Aug. 10, 2012) (“Plaintiffs do not have to plead their evidence to give fair notice of their claims.”); *See also In re Vizio, Inc.*, 238 F. Supp. 3d at 1225-1226 (“Plaintiffs will have to demonstrate that Defendants’ disclosures are ‘reasonably and foreseeably likely to reveal’ what video content Plaintiffs have watched. . . . But this is a factual inquiry ill-suited for resolution on a motion to dismiss.”) (emphasis added).

¹³ Retail analytics firms have used computer and device addresses to pinpoint customer locations— a practice which the Federal Trade Commission (“FTC”) has investigated. *See How to Trace an IP Address to a PC & How to Find Your Own*, <https://www.makeuseof.com/tag/how-to-trace-an-ip-address-how-to-find-your-own-nb/> Given Plaintiffs’ allegations that Defendants employ outside data companies and aggregators (allegations which must be accepted as true with all inferences drawn in Plaintiffs’ favor), it would not be appropriate to conclude that “the linkage of information to identity” here is “too uncertain.” *Yershov*, 820 F.3d. at 486.

At the pleadings stage, the Court must accept as true all allegations of material facts that are in the complaint and must construe all inferences in the light most favorable to the non-moving party.” In re Horizon Healthcare Servs., Inc. Data Breach Litig., 846 F.3d 625 (3d Cir. 2017). Plaintiffs have alleged enough facts to plausibly demonstrate that Defendants have unlawfully disclosed, and are continuing to unlawfully disclose, personal information about consumers that is reasonably and foreseeably likely to reveal, which videos Plaintiffs obtained, where they obtained those videos, and for how long they were watched. “Having informed [Defendants] of the factual basis for their complaint, [Plaintiffs] were required to do no more to stave off threshold dismissal for want of an adequate statement of their claim.” See Johnson v. City of Shelby, Miss., 135 S. Ct. 346, 347 (2014).

For the reasons stated above, Plaintiffs VPPA claims should stand.

B. Plaintiffs’ Wiretap Act Claims Are Well-Pled

The Wiretap Act prohibits “interceptions” of electronic communications. 18 U.S.C. § 2510. It defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” § 2510(4). The “contents” of a communication are defined as “any information concerning the substance, purport, or meaning of that communication.” § 2510(8). Plaintiffs’ complaint alleges enough facts to state a Wiretap Claim that is plausible on its face.

1. Defendants “Intercepted” Electronic Communications.

In order for a communication to be “intercepted” under the Wiretap Act, the communication must be captured contemporaneous with its transmission. See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (“intercept” means “consistent with the ordinary meaning of ‘intercept,’ which is ‘to stop, seize, or interrupt in progress or course before arrival.’”) (citations omitted). Here,

Plaintiffs' Complaint specifically pleads that Defendants captured (and continue to capture) *real-time* viewing behavior data from consumers by means of their Smart TVs. Compl. ¶¶ 41, 53, 63. Moreover, consumers' information was obviously acquired by Defendants during transmission of the programming to Defendants' Smart TVs. How else could Defendants monitor and acquire that information?

These allegations of real-time acquisition are sufficient to withstand a motion to dismiss. See In re Carrier IQ, Inc., 78 F. Supp. 3d 1051, 1078-79 (N.D. Cal. 2015) (denying motion to dismiss Wiretap Act claim where the complaint "references and quotes from a media interview with a Carrier IQ executive" who stated information was provided in real time and holding that the statement "further suggest[s] that the Carrier IQ Software operates contemporaneously with transmissions."); Luis v. Zang, 833 F.3d 619, 630-31 (6th Cir. 2016) (interception sufficiently pled where plaintiff alleged that the product in question "immediately and instantaneously rout[e]s the intercepted communications to their . . . servers" in "near real-time," and *attaching marketing materials* to his complaint that "directly support[ed] an inference of contemporaneous transmission."); Accord In re Google Inc., 806 F.3d 125, 135-140 (3rd Cir. 2015); Campbell v. Facebook, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014). Notably, Plaintiffs here have likewise *attached marketing materials* to their Complaint which clearly and directly supports the exact same inference. See *Automatic Content Software Platform* materials attached to the Amended Complaint as Exhibit 1.

The Complaint plausibly and sufficiently alleges that Defendants took (and continue to take) Plaintiff's and consumers' confidential, identifying information *in real time* while that information was (and is) in transit to Defendants' Smart TVs.

Since the allegations in the Complaint must be accepted as true at this stage, Plaintiffs have sufficiently alleged interception.¹⁴

Plaintiffs have sufficiently alleged interception.

2. Defendants Intercepted The “Contents” Of Communications, As Viewing History And Watching Preferences Are “Contents”

Plaintiffs allege that Defendants intercepted (and continue to intercept) communications between them and cable and satellite providers, streaming devices, and media sources that connect via external input to their Smart TVs and consumers Wifi. Compl. ¶¶ 41-69. Plaintiffs allegations detail that, amongst other confidential, identifying information, Defendants secretly learned what movies and television Plaintiffs and other consumers watch, when they watch, where they watch, and for how long - and then Defendants sold that private information to third parties for profit. *Id.* See also Exhibit 1 to the Complaint. Just as a request in person to a video store clerk for a specific movie is the substance of the message itself, so too are Plaintiffs’ requests for programming through their Smart TVs and other devices, which Defendants intercept. Accord In re Zynga Privacy Litig., 750 F.3d 1098, 2014 WL 1814029, at *9 (9th Cir. 2014) (“[u]nder some circumstances, a user’s request to a search engine for specific information could constitute a communication such that divulging that search term to a third party” could result in disclosure of contents).¹⁵ As alleged in the Complaint, when consumers request a particular program, and Defendants intercept that communication, they are learning specific, highly sensitive information about consumers and consumers’ personal interests.

¹⁴ Carrier IQ correctly distinguished cases involving technology with allegations that the relevant communications were intercepted in real-time, which, is precisely what the Complaint pleads here. 78 F. Supp. 3d at 1078.

¹⁵ In Zynga, the court held that the portion of a webpage request message that provides the address of the webpage from which the request originated did not meet the Wiretap Act’s definition of “contents” because it included only basic identification and address information. The court, however, was careful to say, “Under some circumstances, a user’s request to a search engine for specific information could constitute a communication such that divulging a [Uniform Resource Locator (URL)] containing that search term to a third party could amount to disclosure of the contents of a communication.” 750 F.3d 1098, 1108-09 (emphasis added).

Defendants then sell this confidential, identifying information to target Plaintiffs with ads about their interests – even on devices other than the Smart TV itself. See, e.g., Compl. ¶ 8 (“Unbelievably, Defendants even use their Automatic Content Software, upon information and belief, to push targeted ads to consumers, even on the other separate-unrelated electronic devices that share the same internet network-connection as a Defendants’ Smart TVs. That is, for instance, under Defendants’ set up, a person watching a ‘romantic television program’ on Defendants’ Smart TV in the privacy of their home may then receive advertisements for sexy lingerie on their non-related, separate telephone – even later in time in the workplace.”).

As such, Defendants intercepted, and continue to intercept, under the Wiretap Act. In re Google Inc., 806 F.3d at 135-140.

3. Defendants’ Motion To Dismiss Should Be Denied As To Plaintiffs’ Wiretap Claims

In short, Plaintiffs allege that Defendants’ technology tapped into transmissions to Smart TVs in real time and lifted samples of the content being transmitted so that Defendants could determine what Smart TV-users watch, where they watch, and when they watch. Plaintiffs also allege that Defendants match data and create “fingerprints” of the samples of consumers’ watching history and viewing habits. It does not matter whether the video samples taken by Defendants were fragmentary bits of audio or visual data as opposed to lengthier, wholesale recordings, which will be showcased during discovery in this case. The Wiretap Act prohibits the interception of any information concerning the substance of an electronic communication. 18 U.S.C. § 2510(8) (defining “contents”). There is no safe harbor under the Wiretap Act for interceptions of only parts, or samples, of a communication; nor is there a safe harbor for Smart TVs.

Accordingly, Defendants' motion to dismiss Plaintiffs' Wiretap Act claims should be denied.

C. Defendants' Statute Of Limitations Argument Is Absurd And Incorrect

Defendants' claim that Plaintiffs and the Class should not have their day in Court, and Defendants' should be able to evade responsibility for their alleged misconduct, because "both the VPPA and the Wiretap Act are governed by two-year statutes of limitations" Def. Mem. at 19. Their argument, however, is absurd, as Plaintiffs have alleged an ongoing violation here. That is, Defendants are continuing to engage in the illegal conduct complained of. Accordingly, each time Defendants steal, collect, transmit, sell and/or otherwise use private and/or identifying information about consumers, they violate both statutes. Plain in simple, on its face, there is no valid statute of limitations argument to the Complaint, at all.

Moreover, as alleged by Plaintiffs, concrete news concerning Defendants' misconduct here was first corroborated with "hard evidence" and then made open and available to the public at large at the time of Wikileaks' startling revelation on March 7, 2017, when Wikileaks reported that it had obtained proof in the form of "hard evidence" and government documentation that Smart TVs were in fact being used by outside parties to spy on consumers' private conversations, even when those Smart TVs were supposedly turned off. Compl. § 13. It was that announcement that made Plaintiffs and virtually all consumers throughout the world aware of Defendants' misconduct and specifically, the seriousness of the situation and the need to take legal action against Defendants in this case.

Accordingly, Defendants' contention that Plaintiffs' claims are time barred must fail. These are continuing, ongoing violations by Defendants, and Plaintiffs were first able to reasonably confirm the substance of the allegations in the Complaint in March 2017.

II. Plaintiffs’ Have Thoroughly Documented Exactly What They Have Based Their Allegations On, And Such Allegations Are Not Conclusory

Defendants correctly cite In re Nickelodeon Cons. Priv. Litig., 2014 WL 3012873 (D.N.J. July 2, 2014) and a litany of other case law for the proposition that a court should be “disregarding allegations made ‘upon information and belief’ where no facts pleaded in the complaint support[] the allegations.” Def. Mem. at 7 (citing Nickelodeon, 2014 WL 3012873, at *2 n.3). In this case, however, nothing is further from the truth.

As alleged thoroughly and in detail in the Complaint, Plaintiffs based their allegations on their own experiences and the investigation of counsel. Although not required to do so, Plaintiffs’ Complaint cites almost fifty (50) authorities – including FTC and other reports (see Exhibit 2 to the Amended Complaint); countless news and other articles; the materials and announcements of companies in privity with Defendants, such as Cognitive Networks; and experiences of users. Plaintiffs also attach *two exhibits* to the Complaint which one can reasonably infer directly support Plaintiffs’ allegations here. See Complaint and Exhibits thereto.

Plaintiffs further base their allegations on the extensive investigation conducted by *The Electronic Privacy Information Center* (“EPIC”), a leading consumer group before the FTC (which has also argued to the Supreme Court of the United States), which has independently investigated facts of this case, even filed a related FTC complaint under oath,¹⁶ and EPIC also compiled many statements from consumers regarding the fact that they never knew (or could possibly imagine) that voice recognition system in Smart TVs could intercept transmissions in the home, which Defendants sell to outside third parties. Compl. §92-101. These allegations

¹⁶ See In re: Samsung Electronics Co., Ltd. 20 Federal Trade Commission, February 24, 2015 (attached to the Complaint as Exhibit 2).

contained in EPIC's investigation were confirmed by Plaintiffs' counsel in its own investigation here.

EPIC has already deemed Defendant Samsung's conduct alleged herein to be misleading and deceptive, and has argued to the FTC that "Samsung users could not reasonably have anticipated that by using a voice-controlled Smart TV, their private conversations would be transmitted, sometimes unencrypted, to a third party company." In re: Samsung Electronics Co., Ltd. 20 Federal Trade Commission, February 24, 2015 at 19 (attached to the Complaint as Exhibit 2).

Moreover, Defendants themselves reference Plaintiffs' counsel's diligence in researching and citing the allegations contained in the Complaint, praising that counsel for Plaintiffs' investigation includes "coverage from as early as January 2012." Def. Mem. at 19.

Thus, it is patently false that "no facts pleaded in the complaint support[] the allegations." Nickelodeon, 2014 WL 3012873, at *2 n.3 Rather, Plaintiffs cite overwhelming support for their allegations.

III. The New Jersey Consumer Fraud Act

A. Plaintiffs Have Adequately Pled Violations Of The Consumer Fraud Act

The CFA, N.J. Stat. Ann. § 56:8-2, prohibits:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise

Plaintiffs have properly alleged that “the CFA defines ‘merchandise’ as ‘any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale.’ N.J. Stat. Ann. § 56:8-1(c). . . . and [that] [a]t all relevant times, Defendants have engaged in the advertisement, offering for sale and sale of merchandise within the meaning of N.J. Stat. Ann. § 56:8-1(c), specifically Defendants’ Smart TVs and related services.” Compl. §§ 121-122.

Based on the over one-hundred preceding explanatory paragraphs, Plaintiffs further allege that: (i) “Defendants use A[utomatic] C[ontent] S[oftware]technology to comprehensively collect the sensitive television viewing activity of consumers or households across cable or broadband services, set-top boxes, external streaming devices, DVD players, and over-the-air broadcasts, on a second-by-second basis and store this viewing data indefinitely”; compl. §123; (ii) “Defendants provided this viewing data to third parties, which used it to track and target advertising to individual consumers across devices;” compl. §124 and (iii) “Defendants engaged in these practices through a medium that consumers would not expect to be used for tracking, without consumers’ consent; namely, consumers’ own Smart TVs.” *Id.*

Plaintiffs also properly allege the other requisite elements of their CFA claims, see compl. §§ 118-150, and properly allege that “Defendants’ continued utilization of unlawful and unconscionable marketing practices, and their continuing practice of monitoring, tracking, and reporting viewing habits and personally identifiable information to unauthorized third parties, without consent, constitutes a deceptive act or practice in violation of the CFA [and] such is also an unconscionable commercial practice in violation of the CFA. Each instance of Defendants’ unfair tracking constitutes a separate violation under the CFA, N.J. Stat. Ann. § 56:8-2.” Compl. §125-126, 150.

Plaintiffs further allege that Defendants violated the CFA because they “failed to adequately disclose that the ACS feature of their Smart TVs comprehensively

collected and shared consumers’ television viewing activity from cable boxes, DVRs, streaming devices, and airwaves, which Defendants then provided on a household-by-household basis to third parties (and then to “second-level” third parties).” Compl. §139.

Instead of properly contesting Plaintiffs’ CFA claims, Defendants argue that – even though they avail themselves of New Jersey law as domiciliary companies; and even though these New Jersey companies avail themselves of the benefits associated with New Jersey State Tax law; and even though Defendants could if they wanted to bring a lawsuit themselves against another party under the New Jersey CFA – they themselves (each a New Jersey domiciliary) are not subject to a lawsuit under the CFA for merchandise they produce and sell, and market and advertise in New Jersey because the named Plaintiffs themselves are not from New Jersey. First, such argument seems to be more properly made by Defendants on a motion for certification. Second, Defendants should not be able to use New Jersey law as a shield and a sword. Moreover, Defendants’ argument is belittled by Defendants super-significant contacts with the State of New Jersey and by means of their massive presence and sales, advertising force, and production of TVs in New Jersey.

It is each of Defendants’ super-massive presence in, and contacts with, the State of New Jersey, and the fact that this case is still the pleading stage, that differentiates this situation from the others cases cited by Defendants in this regard.

Defendants also argue that they believe that Florida or maybe New York consumer protection law would better serve this case as applied to them, and contend that the Court should apply one or both of those laws regarding Defendants’ unfair business practices. Def. Mem. at 21-23. As counsel for Defendants know, these laws are modeled after uniform consumer protection laws. If the Court so agrees with Defendants on this point, Plaintiffs will be more than willing to amend the

Complaint and draft allegations against Defendants using the choice-of-law considerations accepted by the Court.¹⁷

B. Particularity Is Not Required With Regard To Non-Fraud Claims, And Since Plaintiffs Have Decided To Voluntarily Withdraw Their Common Law Fraud Claim, Defendants’ Arguments In This Regard Are Rendered Moot

As discussed above and alleged by Plaintiffs in the Complaint, rather than sounding in fraud, as to Plaintiffs’ CFA claims, Plaintiffs have alleged that Defendants utilized unlawful and unconscionable marketing practices, and their continuing practice of monitoring, tracking, recording, and reporting viewing habits and personally identifiable information to unauthorized third parties, without consent, constitutes a deceptive act or practice in violation of the CFA. Plaintiffs also allege that such practices by Defendants constitute an unconscionable commercial practice in violation of the CFA. Compl. §§ 125-126, 150. Plaintiffs do not allege fraud in this regard, just unfair business practices and other misconduct and illegal activity by Defendants that clearly violate the statute. Id.

In addition, Plaintiffs have made the decision to voluntarily withdraw their Common Law Fraud Claims (Count 5) as set forth in the Amended Complaint. See Compl. §§ 179-184. Accordingly, Defendants arguments regarding Plaintiffs’ proper pleading of fraud “particularity” is rendered moot because non-fraud claims do not require such a showing (accord Giercyk v. Nat’l Union Fire Ins. Co. of

¹⁷ Since the filing by Plaintiffs of their Amended Complaint, counsel for Plaintiffs has also been contacted by other individuals currently residing in New Jersey, who bought and used Defendants’ Smart TVs in New Jersey, and who have requested to be considered by counsel for Plaintiffs to join as representative plaintiffs in this lawsuit. Alternatively, should the Court respectfully grant Plaintiffs leave to amend the Complaint, counsel for Plaintiffs will add additional, New Jersey plaintiffs, which will render the instant choice-of-law arguments moot as it relates to a motion to dismiss.

Pittsburgh, 2015 WL 7871165, at *2-3 (D.N.J. 2015) and, for the sake of judicial economy, will not be addressed here.¹⁸

IV. Plaintiffs Do Not Lump; Rather, It Is Defendants That Engage In An Illegal Industry Standard

Defendants also incorrectly state that Plaintiffs' allegations lump Defendants together. Def. Mot. at 25. But Plaintiffs do allege particulars for each Defendant. For instance, Plaintiffs proper differentiate which third party data companies are used by each Defendant. See, e.g., Compl. §§ 43, 44, n.18.

Further, Defendants had licensing agreements with the same outside companies at various times, id., and their data collection and consumer-information mining process was – and is – an *illegal industry standard* that each Defendant reaps many, many tens or hundreds of millions of dollars from. There is so much money at stake here,¹⁹ like swine to the trough, each huge Smart TV manufacturer engaged in virtually the exact same conduct. That is exactly what is alleged by Plaintiffs in the Complaint. For Defendants to try to use their participation in their own illegal industry standard as a defense to the conduct asserted against them by Plaintiffs in this case is ludicrous.

Moreover, Plaintiffs' counsel can ascertain no other logical business purpose for the outside data recognition companies used by Defendants and cited by Plaintiff, than for exactly what Defendants allege about each Defendant in the Complaint. Id. As the old adage goes – “a picture is worth a thousand words” – so counsel for

¹⁸ To the extent the Court requires a showing by Plaintiffs of particularity under Rule 9, Plaintiffs respectfully ask the Court for leave to do so.

¹⁹ See Compl. at n.23. (citing Consumer Reports, Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash, February 27, 2015, <http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm>)

(“**Precise data about consumers TV viewing habits is big business. Revenues for audience-measurement company Nielsen surpassed \$6 Billion last year.**”) (emphasis added).

Plaintiffs respectfully asks this Court to review Exhibit 1 to the Amended Complaint to see that the outside data companies used by Defendants were setting the illegal standards for Defendants to follow, which Defendants happily did.

V. Plaintiffs Unjust Enrichment Claims Are Properly Pled

Plaintiffs believe that the allegations in the Complaint allege a cognizable unjust enrichment claim. Plaintiffs allege based on the preceding 196 paragraphs in the Complaint, that:

- A measurable benefit has been conferred on Defendants under such circumstances that Defendants' retention of the benefit without payment to Plaintiffs and Class Members would be unjust.
- The benefit is the taking of Plaintiffs' and Class Members' private information and capitalizing on it by selling it to third parties for Defendants' monetary gain.
- The benefit is measurable because Defendants' systematically, through carefully designed computer programs and calculations, commoditized and packaged Plaintiffs' and Class Members' private information and sold it to third parties.
- Defendants retained both the private information and profits from its sale.
- Defendants' retention of the benefits would be unjust because this information was private and personal, it contained personally identifiable information, and Plaintiffs and Class Members would not have voluntarily provided that information for free.

Compl. §§ 198-202.

If the reason Defendants believe Plaintiffs' unjust enrichment claim should be dismissed now is because other remedies are available, Courts should not decide at the pleading stage whether an unjust enrichment claim is barred by the availability

of an adequate remedy at law but should defer consideration of that question until subsequent stages of the case. See, e.g., In re Canon Cameras, 2006 WL 1751245, at *2 (S.D.N.Y. June 23, 2006) (New York law). See also Massachusetts v. Mylan Labs., 357 F. Supp. 2d 314, 324 (D. Mass 2005).

VI. Plaintiffs' Have Properly Pled Violations Of The Electronic Communications Privacy Act

Likewise, Plaintiffs believe that their allegations respecting Defendants' violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2512, state a claim on their face. See Compl. §§ 161-178.

In addition the statutory rationales and arguments applied above to Plaintiffs VPPA claim can be used to support Plaintiffs ECPA claims as well. See, supra.

VII. Plaintiffs' Breach of Good Faith and Fair Dealing, Contract Claims, and Express Warranty Claims Are Viable

Simply put, if the Court deems there to be an express, actual, and/or implied agreement between Plaintiffs and members of the Class and the Defendant-manufacturers of the Smart TVs Plaintiffs bought, Plaintiffs have alleged that Defendants, through their unconscionable and illegal practices alleged in the Complaint, have breached those agreements under a variety of theories, including a breach of the implied duty of good faith and fair dealing, breach of express warranty, and breach of contract under a contract-of-adhesion theory. Compl. 185-186, 2-4-205.

Thus, those claims should stand at this pleading stage.

SUMMARY

For the reasons stated above, Defendants' motion to dismiss Plaintiffs'

Amended Class Action Complaint should be dismissed in its entirety.

DATED: March 16, 2018

Respectfully submitted,

By: /s/ Mack Press

Mack Press
BERMAN CLASS LAW
1069 Main Street, suite 136
Holbrook, NY 11741
516-330-7213
mack@mackpress.com